

Practitioner's Docket No.: 008312-0305943
Client Reference No.: T4KM-03S0231-1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: HIROTSUGU KATO, Confirmation No: UNKNOWN
et al.

Application No.:

Group No.:

Filed: September 12, 2003

Examiner: UNKNOWN

For: TRANSMITTER APPARATUS, RECEIVER APPARATUS AND RECEIVING
METHOD

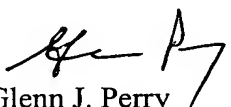
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBMISSION OF PRIORITY DOCUMENT

Attached please find the certified copy of the foreign application from which priority is
claimed for this case:

<u>Country</u>	<u>Application Number</u>	<u>Filing Date</u>
Japan	2002-340968	11/25/2002

Date: September 12, 2003
PILLSBURY WINTHROP LLP
P.O. Box 10500
McLean, VA 22102
Telephone: (703) 905-2000
Facsimile: (703) 905-2500
Customer Number: 00909


Glenn J. Perry
Registration No. 28458

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年11月25日

出 願 番 号

Application Number:

特願2002-340968

[ST.10/C]:

[JP2002-340968]

出 願 人

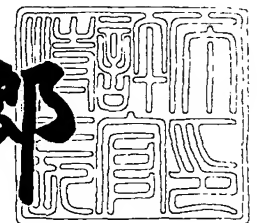
Applicant(s):

株式会社東芝

2003年 3月28日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3021546

【書類名】 特許願

【整理番号】 A000204741

【提出日】 平成14年11月25日

【あて先】 特許庁長官 殿

【国際特許分類】 H04N 7/00

【発明の名称】 送信装置、受信装置及び受信方法

【請求項の数】 12

【発明者】

 【住所又は居所】 東京都青梅市末広町2丁目9番地 株式会社東芝青梅事業所内

 【氏名】 加藤 尋嗣

【発明者】

 【住所又は居所】 東京都青梅市末広町2丁目9番地 株式会社東芝青梅事業所内

 【氏名】 安木 成次郎

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

 【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 送信装置、受信装置及び受信方法

【特許請求の範囲】

【請求項 1】 暗号化されたコンテンツにリンク情報を付加して送信する第 1 の送信手段と、

この第 1 の送信手段で送信されたリンク情報を用いて生成され、通信ネットワークを介して入力される上りデータに基づいて、前記第 1 の送信手段で送信されたコンテンツを復号するための暗号鍵を、前記通信ネットワーク上に送信する第 2 の送信手段とを具備してなることを特徴とする送信装置。

【請求項 2】 コンテンツを所定のデータ量を有するデータ単位に分割し、この分割された各データ単位に対してそれぞれ異なる暗号鍵を用いて暗号化処理を施し、この暗号化された各データ単位に対してそれぞれ再生タイミングを示す時間情報を付加し、この時間情報が付加され暗号化された各データ単位を連続させた暗号化コンテンツにリンク情報を付加して送信する第 1 の送信手段と、

この第 1 の送信手段で送信されたリンク情報を用いて生成され、通信ネットワークを介して入力される上りデータに基づいて、前記第 1 の送信手段で送信された暗号化コンテンツのデータ単位を指定するための時間情報と、この時間情報に対応するデータ単位を復号するための暗号鍵とを、前記通信ネットワーク上に送信する第 2 の送信手段とを具備してなることを特徴とする送信装置。

【請求項 3】 前記第 1 の送信手段は放送局であり、前記第 2 の送信手段はインターネットに接続されたサーバであることを特徴とする請求項 1 または 2 記載の送信装置。

【請求項 4】 前記第 2 の送信手段は、前記第 1 の送信手段で送信された暗号化コンテンツの各データ単位をそれぞれ指定するための時間情報と、この時間情報に対応するデータ単位を復号するための暗号鍵とが対応付けられて記録された記録手段を備えていることを特徴とする請求項 2 記載の送信装置。

【請求項 5】 暗号化されたコンテンツをリンク情報とともに受信して蓄積する記録手段と、

この記録手段に蓄積されたリンク情報に基づいて、前記暗号化コンテンツを復

号するための暗号鍵を要求する上りデータを生成し、通信ネットワーク上に送信する送信手段と、

前記通信ネットワーク上から前記上りデータで要求した暗号鍵を取得し、前記記録手段に蓄積された暗号化コンテンツを復号する復号手段とを具備してなることを特徴とする受信装置。

【請求項 6】 分割されたデータ単位毎にそれぞれ異なる暗号鍵を用いて暗号化処理が施され、この暗号化された各データ単位毎にそれぞれ再生タイミングを示す時間情報が付加されてなる暗号化コンテンツを、リンク情報とともに受信して蓄積する記録手段と、

この記録手段に蓄積されたリンク情報に基づいて、前記暗号化コンテンツを各データ単位毎に復号するための時間情報と暗号鍵とを要求する上りデータを生成し、通信ネットワーク上に送信する送信手段と、

前記通信ネットワーク上から前記上りデータで要求した時間情報と暗号鍵とを取得し、前記記録手段に蓄積された暗号化コンテンツに対して、前記取得した時間情報で示されるデータ単位を復号する復号手段とを具備してなることを特徴とする受信装置。

【請求項 7】 前記記録手段に蓄積された複数の暗号化コンテンツのタイトルを画面上に一覧表示し、該画面上で選択させる操作手段を具備してなることを特徴とする請求項 5 または 6 記載の受信装置。

【請求項 8】 前記操作手段で選択されたタイトルに対応する暗号化コンテンツに対して、少なくとも再生、停止、一時停止及び特殊再生のいずれかを要求するための操作画面を表示する表示手段を具備してなることを特徴とする請求項 7 記載の受信装置。

【請求項 9】 暗号化されたコンテンツをリンク情報とともに受信する工程と、

受信した暗号化コンテンツ及びリンク情報を蓄積する工程と、

蓄積されたリンク情報に基づいて、前記暗号化コンテンツを復号するための暗号鍵を要求する上りデータを生成する工程と、

生成された上りデータを通信ネットワーク上に送信する工程と、

前記通信ネットワーク上から前記上りデータで要求した暗号鍵を取得する工程と、

取得した暗号鍵に基づいて前記蓄積された暗号化コンテンツを復号する工程とを具備してなることを特徴とする受信方法。

【請求項 1 0】 分割されたデータ単位毎にそれぞれ異なる暗号鍵を用いて暗号化処理が施され、この暗号化された各データ単位毎にそれぞれ再生タイミングを示す時間情報が付加されてなる暗号化コンテンツを、リンク情報とともに受信する工程と、

受信した暗号化コンテンツ及びリンク情報を蓄積する工程と、

蓄積されたリンク情報に基づいて、前記暗号化コンテンツを各データ単位毎に復号するための時間情報と暗号鍵とを要求する上りデータを生成する工程と、

生成された上りデータを通信ネットワーク上に送信する工程と、

前記通信ネットワーク上から前記上りデータで要求した時間情報と暗号鍵とを取得する工程と、

取得した時間情報で示されるデータ単位を、取得した暗号鍵を用いて復号する工程とを具備してなることを特徴とする受信方法。

【請求項 1 1】 前記蓄積された複数の暗号化コンテンツのタイトルを画面上に一覧表示する工程と、

一覧表示されたタイトルを画面上で選択させる工程とを具備してなることを特徴とする請求項 9 または 1 0 記載の受信方法。

【請求項 1 2】 前記選択されたタイトルに対応する暗号化コンテンツに対して、少なくとも再生、停止、一時停止及び特殊再生のいずれかを要求するための操作画面を表示する工程を具備してなることを特徴とする請求項 1 1 記載の受信方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、テレビジョン放送と例えばインターネット等のネットワークとによるデータコンテンツの送信が可能な送信装置の改良に関する。また、この発明

は、上記の送信装置で送信されたデータコンテンツを受信する受信装置及び受信方法の改良に関する。

【 0 0 0 2 】

【従来の技術】

周知のように、近年では、多種多様な情報供給メディアから得られるコンテンツを、多数のユーザに提供するための配信システムが開発されている。このようなコンテンツ配信システムとして、現在では、例えば動画コンテンツ配信サービス等が実用化されている。

【 0 0 0 3 】

この動画コンテンツ配信サービスは、テレビジョン放送受信機をインターネットに接続し、テレビジョン放送受信機からインターネット上の所定のサーバに動画コンテンツの呼び出しを要求することにより、サーバから動画コンテンツがテレビジョン放送受信機に配信されて視聴されるようにしたものである。

【 0 0 0 4 】

ところで、上記のような動画コンテンツの配信サービスでは、通信回線を流れる動画コンテンツのデータサイズが非常に大きなものとなる。このため、ユーザに対して、十分に実用的なレベルでの動画コンテンツの配信サービスを提供するためには、ネットワークの高速化（ブロードバンド化）が必要になる。

【 0 0 0 5 】

例えば、動画コンテンツにMPEG（Moving Picture Experts Group）2方式での圧縮処理を施した場合、その伝送速度は、NTSC（National Television System Committee）方式による標準テレビジョン画質で4Mbps（Mega bit per second）、ハイビジョン画質で30Mbpsに及ぶことがある。

【 0 0 0 6 】

これに対し、一般家庭におけるアナログ電話回線で、アナログモデムによるインターネット通信を行なう場合、その伝送速度は、最大でも56Kbps（Kilo bit per second）程度である。

【 0 0 0 7 】

このような状況で、例えば、NTSC方式による標準テレビジョン画質で1時

間分の動画コンテンツを、サーバからテレビジョン放送受信機にダウンロードした場合、1時間分の動画コンテンツの全データサイズは、 $4\text{ Mbps} \times 1\text{ 時間} \times 60\text{ 分} \times 60\text{ 秒} = 14400\text{ Mbit} = 14745600\text{ Kbit}$ となる。

【0008】

このため、このデータをダウンロードするのに要する時間は、 $14745600\text{ Kbit} / 56\text{ Kbps} = 263314\text{ 秒} = 73\text{ 時間}$ 、すなわち、3日かかることになる。つまり、ユーザの要求に応じて、サーバから動画コンテンツをダウンロードし、視聴を行なうことは実用上不可能なこととなる。

【0009】

また、最近では、アナログ電話回線を用いたブロードバンド通信サービスとして、ADSL (Asymmetric Digital Subscriber Line) が普及している。このADSLによるインターネット接続では、 $1.5\text{ Mbps} \sim 12\text{ Mbps}$ の伝送レートが得られる。

【0010】

このため、ADSLの8Mbpsタイプの場合、NTSC方式による標準テレビジョン画質である4Mbpsの動画コンテンツに対しては、その再生を行なえるだけの通信性能を確保することができる可能性がある。ところが、30Mbps近い伝送速度を必要とするハイビジョン画質の動画コンテンツでは、さらに3倍から4倍の伝送速度が必要になる。

【0011】

なお、FTTH (Fiber To The Home) を用いた光ファイバ通信手段は、100Mbpsの伝送速度が得られるため、30Mbps近い伝送速度のハイビジョン画質の動画コンテンツを、安定して再生することができる。ところが、FTTHの普及には、通信基盤 (infrastructure) の整備が必要であることから、一般家庭においては、当面、ADSL等のアナログ電話回線を使用したインターネット接続が主流になると考えられている。

【0012】

したがって、動画コンテンツ配信サービスの提供者 (プロバイダ) は、幅広くユーザを獲得するために、アナログ電話回線でインターネットへの接続を行なっ

ている多数の一般家庭に対しても、実用的なサービスの提供を行なえるようにする必要があり、そのために、低伝送速度に対応した低画質の動画コンテンツを用意している。

【 0 0 1 3 】

ただし、通信ネットワークの伝送速度は、ベストエフォートと称され保証されているものではなく、例えば、A D S L の 8 Mbps タイプであっても、ネットワークの輻輳時には著しく伝送速度が低下する。この場合、テレビジョン放送受信機においては、動画コンテンツの受信エラーにより再生画像が破綻する事態が発生する。

【 0 0 1 4 】

このため、プロバイダは、テレビジョン放送受信機側で動画コンテンツの受信が安定して行なわれるようにするため、通信ネットワークの伝送速度が低下することを予め考慮し、動画コンテンツのデータサイズを極力小さくして、通信ネットワークの伝送速度に対して余裕を持たせたサービスを行なう必要がある。これにより、提供することができる動画コンテンツは低品質のものとなる。

【 0 0 1 5 】

このように、一般家庭におけるインターネット接続環境の高速化が十分に実現できないことには、高画質な動画コンテンツを配信するのに十分な伝送速度を確保できないこととなり、動画コンテンツ配信サービスを行なう上での大きな制約となっている。

【 0 0 1 6 】

なお、特許文献 1 として提示する特開 2 0 0 2 - 6 4 8 0 6 号公報には、テレビジョン放送信号に付加されたパスワードデータと、テレビジョン放送信号に付加されたアドレスによりインターネットを介して得られたパスワードデータとが対応したとき、テレビジョン放送で配信されたコンテンツを受信機に正常に表示する技術が開示されている。

【 0 0 1 7 】

また、特許文献 2 として提示する特開 2 0 0 2 - 5 5 9 0 9 号公報には、受信装置が、受信したコンテンツからインターネットアドレスを抽出してリモートコ

ントローラに記憶させると、アクセス装置が、リモートコントローラからインターネットアドレスを読み取って表示するので、ユーザがインターネットアドレスを選択して所望のサイトにアクセス可能とする技術が開示されている。

【0018】

しかしながら、これらの特許文献1及び2には、いずれも、上記したように、データサイズが非常に大きな動画コンテンツを、ユーザに対して十分に実用的となる伝送速度での配信サービスができるようにすることについては、何らの記載もなされていないものである。

【0019】

【特許文献1】

特開2002-64806号公報

【0020】

【特許文献2】

特開2002-55909号公報

【0021】

【発明が解決しようとする課題】

以上のように、現状における動画コンテンツの配信システムでは、ハイビジョンのような大容量の動画コンテンツを配信するためには、ユーザ側に高速な通信回線が必要となる。

【0022】

しかしながら、現状の一般家庭におけるネットワーク接続環境は、アナログ電話回線が主流であることから、動画コンテンツのダウンロードを行なうための十分な伝送速度を確保することができないことになる。特に、ハイビジョンレベルの高画質動画コンテンツをダウンロードして再生することは困難である。

【0023】

このため、プロバイダは、低速の通信回線を持つユーザに対しても、配信サービスを提供することができるように、低レート of 動画コンテンツを配信しなければならないという問題を有している。

【0024】

そこで、この発明は上記事情を考慮してなされたもので、ユーザのネットワーク接続環境に無関係に、大容量のデータコンテンツを実用的なレベルで安定に配信することを可能とした送信装置、受信装置及び受信方法を提供することを目的とする。

【 0 0 2 5 】

【課題を解決するための手段】

この発明に係る送信装置は、暗号化されたコンテンツにリンク情報を付加して送信する第1の送信手段と、この第1の送信手段で送信されたリンク情報を用いて生成され、通信ネットワークを介して入力される上りデータに基づいて、第1の送信手段で送信されたコンテンツを復号するための暗号鍵を、通信ネットワーク上に送信する第2の送信手段とを備えるようにしたものである。

【 0 0 2 6 】

また、この発明に係る受信装置は、暗号化されたコンテンツをリンク情報とともに受信して蓄積する記録手段と、この記録手段に蓄積されたリンク情報に基づいて、暗号化コンテンツを復号するための暗号鍵を要求する上りデータを生成し、通信ネットワーク上に送信する送信手段と、通信ネットワーク上から上りデータで要求した暗号鍵を取得し、記録手段に蓄積された暗号化コンテンツを復号する復号手段とを備えるようにしたものである。

【 0 0 2 7 】

さらに、この発明に係る受信方法は、暗号化されたコンテンツをリンク情報とともに受信する工程と、受信した暗号化コンテンツ及びリンク情報を蓄積する工程と、蓄積されたリンク情報に基づいて、暗号化コンテンツを復号するための暗号鍵を要求する上りデータを生成する工程と、生成された上りデータを通信ネットワーク上に送信する工程と、通信ネットワーク上から上りデータで要求した暗号鍵を取得する工程と、取得した暗号鍵に基づいて蓄積された暗号化コンテンツを復号する工程とを備えるようにしたものである。

【 0 0 2 8 】

上記のような構成及び方法によれば、大容量のデータコンテンツは暗号化してリンク情報とともに送信して受信側で蓄積し、通信ネットワークでは暗号を解く

ための暗号鍵を送信するようにしている。これにより、通信ネットワークを使用して大容量のコンテンツを配信する必要がなくなるので、ユーザのネットワーク接続環境に関係なく、大容量のコンテンツを実用的なレベルで安定に配信して視聴させることが可能となる。

【 0 0 2 9 】

【発明の実施の形態】

以下、この発明の実施の形態について、図面を参照して詳細に説明する。図 1 は、この実施の形態で説明する動画コンテンツ配信システムを概略的に示している。図 1 において、符号 1 1 は放送局である。この放送局 1 1 は、動画コンテンツをデジタル放送している。

【 0 0 3 0 】

この場合、放送局 1 1 は、放送する動画コンテンツに暗号化処理を施すとともに、特定のサーバ 1 2 にアクセスして情報を読み出すためのリンク情報を付加して、アンテナ 1 3 から送信している。また、この放送局 1 1 は、動画コンテンツの暗号化に使用した暗号鍵を、上記リンク情報で特定されるサーバ 1 2 に供給し保持させる。

【 0 0 3 1 】

ここで、放送局 1 1 のアンテナ 1 3 から送信された信号は、衛星 1 4 を介してユーザの持つテレビジョン放送受信機 1 5 のアンテナ 1 6 に受信される。このテレビジョン放送受信機 1 5 は、アンテナ 1 6 で受信された信号から動画コンテンツを取り出し、暗号化されたままの状態 HDD (Hard Disk Drive) 1 7 に供給し、そのハードディスク 1 8 に蓄積する。

【 0 0 3 2 】

また、このテレビジョン放送受信機 1 5 は、アンテナ 1 6 で受信された信号からリンク情報を取り出し、インターネット 1 9 を介してサーバ 1 2 にアクセスすることにより、該サーバ 1 2 から暗号鍵を取得する。

【 0 0 3 3 】

このため、テレビジョン放送受信機 1 5 では、ハードディスク 1 8 から暗号化された動画コンテンツを読み出し、サーバ 1 2 から取得した暗号鍵に基づいて動

画コンテンツの暗号化を解くことにより、動画コンテンツを視聴することが可能となる。

【 0 0 3 4 】

上記した実施の形態によれば、大容量のデータコンテンツである動画コンテンツは、暗号化して放送電波によりテレビジョン放送受信機 1 5 に送信してハードディスク 1 8 に蓄積し、インターネット 1 9 では動画コンテンツの暗号を解くための暗号鍵を送信するようにしている。

【 0 0 3 5 】

これにより、インターネット 1 9 上で大容量の動画コンテンツを配信する必要がなくなるので、アナログ電話回線でインターネット 1 9 への接続を行なっている一般のユーザに対しても、大容量の動画コンテンツを実用的なレベルで安定に配信して視聴させることが可能となる。

【 0 0 3 6 】

ここで、図 2 (a) ~ (d) は、動画コンテンツを暗号化する手法を説明している。すなわち、図 2 (a) に示すように、連続する一連の動画コンテンツを、同図 (b) に示すように、複数の動画パケット P 1 , P 2 , P 3 , P 4 , …… , P n に分割する。

【 0 0 3 7 】

そして、図 2 (c) に示すように、分割された各動画パケット P 1 , P 2 , P 3 , P 4 , …… , P n に対して、それぞれ異なる暗号鍵 K 1 , K 2 , K 3 , K 4 , …… , K n を用いた暗号化処理が施される。

【 0 0 3 8 】

また、この暗号化された各動画パケット C 1 , C 2 , C 3 , C 4 , …… , C n に対して、それぞれ再生するタイミングを指定するための時間情報であるタイムスタンプ T 1 , T 2 , T 3 , T 4 , …… , T n が付加される。

【 0 0 3 9 】

その後、タイムスタンプ T 1 , T 2 , T 3 , T 4 , …… , T n 付きの暗号化動画パケット C 1 , C 2 , C 3 , C 4 , …… , C n が、図 2 (d) に示すように、連続する一連の暗号化動画コンテンツに再構成され、ここに、動画コンテンツの

暗号化処理が完了される。

【 0 0 4 0 】

この場合、上記放送局 1 1 では、図 2 (d) に示すように構成された暗号化動画コンテンツに、サーバ 1 2 にアクセスするためのリンク情報を付加して、アンテナ 1 3 から送信している。

【 0 0 4 1 】

また、放送局 1 1 では、動画コンテンツの暗号化処理に使用した暗号鍵 K 1 , K 2 , K 3 , K 4 , …… , K n と、タイムスタンプ T 1 , T 2 , T 3 , T 4 , …… , T n とを対応させて、サーバ 1 2 に供給し保持させている。

【 0 0 4 2 】

そして、上記放送局 1 1 からアンテナ 1 3 を介して送信された暗号化動画コンテンツとリンク情報とは、テレビジョン放送受信機 1 5 で受信されハードディスク 1 8 に蓄積される。

【 0 0 4 3 】

ここで、ユーザが、テレビジョン放送受信機 1 5 に対して、ハードディスク 1 8 に蓄積されている所定の暗号化動画コンテンツの視聴を要求する操作を行なった場合、テレビジョン放送受信機 1 5 は、視聴が要求された暗号化動画コンテンツに対応するリンク情報をハードディスク 1 8 から読み出す。

【 0 0 4 4 】

そして、テレビジョン放送受信機 1 5 は、読み出したリンク情報に基づいて、暗号化動画コンテンツを復号するための暗号鍵 K 1 , K 2 , K 3 , K 4 , …… , K n を要求するコマンドを生成し、上りデータとしてインターネット 1 9 上に送信する。

【 0 0 4 5 】

この上りデータには、必要な暗号鍵 K 1 , K 2 ; K 3 , K 4 , …… , K n を保持しているサーバ 1 2 を特定するための I P (Internet Protocol) アドレスが付加されている。

【 0 0 4 6 】

このため、 I P アドレスに対応するサーバ 1 2 は、上りデータに含まれている

暗号鍵要求コマンドを受信すると、自己の保持している暗号鍵 K_1 , K_2 , K_3 , K_4 , …… , K_n とタイムスタンプ T_1 , T_2 , T_3 , T_4 , …… , T_n とを含む復号用データを、インターネット 19 上に送信する。

【 0 0 4 7 】

この場合、サーバ 12 は、暗号鍵 K_1 とタイムスタンプ T_1 とのペア、暗号鍵 K_2 とタイムスタンプ T_2 とのペア、暗号鍵 K_3 とタイムスタンプ T_3 とのペア、……というように、各ペアを所定のタイミングで順次インターネット 19 上に送信している。

【 0 0 4 8 】

これにより、テレビジョン受信機 15 は、まず、暗号鍵 K_1 とタイムスタンプ T_1 とのペアを取得し、ハードディスク 18 に蓄積された暗号化動画コンテンツの中から、タイムスタンプ T_1 と一致する暗号化動画パケット $T_1 + C_1$ を読み出す。

【 0 0 4 9 】

その後、テレビジョン受信機 15 は、タイムスタンプ T_1 とペアで取得された暗号鍵 K_1 を使用して、暗号化動画パケット C_1 に復号化処理を施し、タイムスタンプ T_1 を削除して動画パケット P_1 を得る。

【 0 0 5 0 】

次に、テレビジョン受信機 15 は、暗号鍵 K_2 とタイムスタンプ T_2 とのペアを取得し、ハードディスク 18 に蓄積された暗号化動画コンテンツの中から、タイムスタンプ T_2 と一致する暗号化動画パケット $T_2 + C_2$ を読み出す。

【 0 0 5 1 】

その後、テレビジョン受信機 15 は、タイムスタンプ T_2 とペアで取得された暗号鍵 K_2 を使用して、暗号化動画パケット C_2 に復号化処理を施し、タイムスタンプ T_2 を削除して動画パケット P_2 を得る。以下、同様な動作が、動画コンテンツ P_n が得られるまで繰り返される。

【 0 0 5 2 】

すなわち、テレビジョン受信機 15 は、復号用データとして取得した暗号鍵 K_i ($1 \leq i \leq n$) とタイムスタンプ T_i とのペアによって、ハードディスク 18

に蓄積された暗号化動画コンテンツの中から、タイムスタンプ T_i と一致する暗号化動画パケット $T_i + C_i$ を読み出す。

【0053】

そして、テレビジョン受信機15は、タイムスタンプ T_i とペアで取得された暗号鍵 K_i を使用して、暗号化動画パケット C_i に復号化処理を施し、タイムスタンプ T_i を削除して動画パケット P_i を得る。

【0054】

その後、テレビジョン放送受信機15は、上記のようにして得られた各動画パケット $P_1, P_2, P_3, P_4, \dots, P_n$ から、図2(a)に示したような連続する一連の動画コンテンツを構成し、この動画コンテンツを復調して映像表示することができる。

【0055】

上記したように、連続する一連の動画コンテンツを複数の動画パケット $P_1, P_2, P_3, P_4, \dots, P_n$ に分割し、各動画パケット $P_1, P_2, P_3, P_4, \dots, P_n$ に対して、それぞれ異なる暗号鍵 $K_1, K_2, K_3, K_4, \dots, K_n$ を用いて暗号化処理を施すことにより、動画コンテンツの秘匿性をより一層高めることができる。

【0056】

図3は、上記したサーバ12及びテレビジョン放送受信機15の詳細を示している。すなわち、サーバ12は、放送局11から送出された暗号鍵 K_i とタイムスタンプ T_i とを、メモリ20に記録している。この場合、メモリ20には、図4に示すように、暗号鍵 $K_1, K_2, K_3, K_4, \dots, K_n$ とタイムスタンプ $T_1, T_2, T_3, T_4, \dots, T_n$ とが対応付けられて記録される。

【0057】

このメモリ20に記録された暗号鍵 K_i とタイムスタンプ T_i とは、制御部21の指示に基づいて制御される読み出し部22により選択的に読み出される。この読み出された暗号鍵 K_i とタイムスタンプ T_i とは、エンコーダ23でインターネット19に出力するための形態に変換され、上記復号化データとして送信部24を介してインターネット19上に送信される。

【0058】

また、サーバ12は、テレビジョン放送受信機15からインターネット19上に送信された上りデータを受信し、デコーダ25でデコード処理した後、上記制御部21により解析して読み出し部22を制御している。

【0059】

一方、上記テレビジョン放送受信機15において、アンテナ16で受信した信号は、チューナ部26に供給されて所定の暗号化動画コンテンツとそれに付加されたリンク情報とが抽出される。

【0060】

このチューナ部26で抽出された暗号化動画コンテンツとリンク情報とは、復調部27で復調処理が施された後、ファイルシステム部28を介してHDD17に送出され、ハードディスク18に記録される。

【0061】

ユーザは、リモートコントローラ29を操作することにより、テレビジョン放送受信機15に対して、ハードディスク18に記録された暗号化動画コンテンツの視聴を要求することができる。この場合、リモートコントローラ29では、タイムスタンプを指定して暗号化動画コンテンツの再生を要求する。

【0062】

リモートコントローラ29の操作情報を受けたUI (User Interface) 部30は、ファイルシステム部28を介して視聴要求された暗号化動画コンテンツに付加されているリンク情報をハードディスク18から読み出す。

【0063】

そして、UI部30は、該リンク情報に基づいて、リモートコントローラ29で指定されたタイムスタンプに対応する暗号鍵を要求するコマンドを含む上りデータを生成する。この上りデータは、エンコーダ31によりインターネット19に出力するための形態に変換され、インターネット19上に送信される。

【0064】

すると、上記サーバ12では、インターネット19上に送信された上りデータからタイムスタンプ付きの暗号鍵要求コマンドを受信し、デコーダ25でデコー

ド処理して制御部 2 1 に供給する。

【 0 0 6 5 】

制御部 2 1 では、入力されたタイムスタンプに基づいて読み出し部 2 2 を制御し、メモリ 2 0 から指定のタイムスタンプ T_i とそれに対応する暗号鍵 K_i とを読み出させる。そして、この読み出し部 2 2 で読み出されたタイムスタンプ T_i と暗号鍵 K_i とは、前述したように復号用データとして、エンコーダ 2 3 及び送信部 2 4 を介してインターネット 1 9 上に送信される。

【 0 0 6 6 】

すると、テレビジョン放送受信機 1 5 では、インターネット 1 9 上に送信された復号用データを受信部 3 2 で受信し、デコーダ 3 3 でデコード処理した後、分離部 3 4 によりタイムスタンプ T_i と暗号鍵 K_i とに分離する。そして、タイムスタンプ T_i は、ファイルシステム部 2 8 に供給され、暗号鍵 K_i は、復号部 3 5 に供給される。

【 0 0 6 7 】

この場合、ファイルシステム部 2 8 は、入力されたタイムスタンプ T_i に対応する暗号化動画パケット $T_i + C_i$ をハードディスク 1 8 から読み取り、復号部 3 5 に供給する。そして、復号部 3 5 は、入力された暗号化動画パケット C_i に対して、分離部 3 4 から供給された暗号鍵 K_i を用いて復号化処理を施し、動画パケット P_i を生成する。

【 0 0 6 8 】

その後、復号部 3 5 で生成された動画パケット P_i は、デコーダ 3 6 に供給されてデコード処理されることにより連続する一連の動画コンテンツに構成された後、モニタ 3 7 で映像表示される。

【 0 0 6 9 】

次に、ユーザが、リモートコントローラ 2 9 を用いて、ハードディスク 1 8 に記録されている複数の暗号化動画コンテンツの中から、所望の暗号化動画コンテンツに対して視聴要求を行なう手法について説明する。

【 0 0 7 0 】

まず、ユーザが、リモートコントローラ 1 8 の再生要求キーを操作すると、フ

ファイルシステム部 2 8 は、ハードディスク 1 8 に記録されている複数の暗号化動画コンテンツをジャンル別にモニタに 3 7 に表示する。

【 0 0 7 1 】

ユーザが、モニタ 3 7 の画面上で、例えば、映画のジャンルを選択すると、図 5 (a) に示すように、ハードディスク 1 8 に記録されている複数の暗号化動画コンテンツの中から、映画に対応するコンテンツのサムネイル画面とタイトルとそのリンク情報であるアドレスとが、モニタ 3 7 上に一覧表示される。

【 0 0 7 2 】

なお、映画に対応するコンテンツが一画面で表示し切れない場合には、モニタ 3 7 上に「戻る」及び「次へ」等の操作エリアが表示され、複数の画面に渡って切り替えて表示されるようになる。

【 0 0 7 3 】

この一覧表示画面において、1つのタイトルが枠線 L で囲まれている。この枠線 L は、リモートコントローラ 2 9 の上下キー等进行操作することにより、他のタイトルを囲むように上下移動される。そして、ユーザは、所望のタイトルを枠線 L で囲み、リモートコントローラ 2 9 の決定キー进行操作することによって、図 5 (b) に示すように、そのタイトルの映画に対応する操作画面がモニタ 3 7 上に表示される。

【 0 0 7 4 】

この操作画面においては、再生 P L A Y 、早送り F F 、早戻し R E W 、一時停止 P A U S E 及び停止 S T O P の操作が可能になっている。これらの操作も、リモートコントローラ 2 9 の左右キー等进行操作して選択し、決定キー进行操作することで実現される。

【 0 0 7 5 】

例えば、再生 P L A Y が操作されると、前述したように、テレビジョン放送受信機 1 5 の U I 部 3 0 は、選択された暗号化動画コンテンツを構成する全ての暗号化動画パケット T i + C i を順次指定する上りデータをインターネット 1 9 上に送信する。

【 0 0 7 6 】

このため、サーバ 1 2 の制御部 2 1 は、上りデータで指定されたタイムスタンプ T_i と暗号鍵 K_i とを、順次復号用データとしてインターネット 1 9 上に送信する。

【 0 0 7 7 】

これにより、テレビジョン放送受信機 1 5 では、復号用データに基づいて、ハードディスク 1 8 から暗号化動画パケット C_i を順次読み出して復号化し、ここに、ハードディスク 1 8 に記録された複数の暗号化動画コンテンツの中から、ユーザの選択したコンテンツを再生することができる。

【 0 0 7 8 】

具体的に言えば、図 6 (a) は、ハードディスク 1 8 に記録された複数の暗号化動画コンテンツの中から、ユーザがリモートコントローラ 2 9 を操作して視聴することを選択したコンテンツ $T_i + C_i$ を示している。

【 0 0 7 9 】

テレビジョン放送受信機 1 5 では、サーバ 2 1 から送信された復号用データに含まれるタイムスタンプ T_i に基づいて、図 6 (b) に示すように、タイムスタンプ T_1, T_2, T_3, \dots に対応する暗号化動画パケット C_1, C_2, C_3, \dots を、順次ハードディスク 1 8 から読み出すとともに、暗号鍵 K_1, K_2, K_3, \dots に基づいて復号化する。

【 0 0 8 0 】

そして、テレビジョン放送受信機 1 5 では、図 6 (c) に示すように、復号後の動画パケット P_1, P_2, P_3, \dots を連続させて動画コンテンツを構成することにより、動画コンテンツの再生を行なうことができる。

【 0 0 8 1 】

また、このような再生中に、例えば、動画パケット P_4 の再生時に一時停止 $PAUSE$ が操作されると、その動画パケット P_4 に対応するタイムスタンプ T_4 を指定する上りデータがインターネット 1 9 上に送信される。

【 0 0 8 2 】

この上りデータを受けたサーバ 1 2 は、一時停止 $PAUSE$ の操作が解除されるまで、動画パケット P_4 に対応するタイムスタンプ T_4 とその暗号鍵 K_4 とを

復号用データに含めて出力し続ける。

【 0 0 8 3 】

これにより、テレビジョン放送受信機 1 5 では、ハードディスク 1 8 からタイムスタンプ T 4 に対応する暗号化動画パケット C 4 のみが読み取られるようになる。そして、この暗号化動画パケット C 4 が暗号鍵 K 4 で復号化されて動画パケット P 4 となり、図 6 (c) に示すように連続的に再生されるようになって、ここに、一時停止機能が行なわれることになる。

【 0 0 8 4 】

また、再生 P L A Y と早送り F F とが共に操作されて早送り再生（特殊再生）が要求されると、テレビジョン放送受信機 1 5 は、図 7 (a) に示すようにハードディスク 1 8 に記録された暗号化動画コンテンツの中から、タイムスタンプ T 1 , T 4 , T 7 , ……を間欠的に指定する上りデータをインターネット 1 9 に送信する。

【 0 0 8 5 】

これにより、サーバ 1 2 は、タイムスタンプ T 1 , T 4 , T 7 , ……と、その暗号鍵 K 1 , K 4 , K 7 , ……とを含む復号用データを送信し、テレビジョン放送受信機 1 5 は、受信した復号用データに基づいて、図 7 (b) に示すように、飛び飛びに暗号化動画パケット C 1 , C 4 , C 7 , ……をハードディスク 1 8 から読み出して、暗号鍵 K 1 , K 4 , K 7 , ……により復号化する。

【 0 0 8 6 】

そして、テレビジョン放送受信機 1 5 は、復号化された動画パケット P 1 , P 4 , P 7 , ……を、図 7 (c) に示すように連続的に再生し、ここに、早送り再生が実現されることになる。

【 0 0 8 7 】

なお、再生 P L A Y と早戻し R E W とが共に操作されて早戻し再生（特殊再生）が要求された場合にも、タイムスタンプ T i を過去に向けて間欠的に指定することにより、容易に実現することができる。

【 0 0 8 8 】

さらに、スロー再生（特殊再生）が要求された場合、テレビジョン放送受信機

15は、図8(a)に示すようにハードディスク18に記録された暗号化動画コンテンツの中から、タイムスタンプT1, T2, T3, ……を順次指定する上りデータをインターネット19に送信する。

【0089】

これにより、サーバ12は、タイムスタンプT1, T2, T3, ……と、その暗号鍵K1, K2, K3, ……とを含む復号用データを送信し、テレビジョン放送受信機15は、受信した復号用データに基づいて、図8(b)に示すように、暗号化動画パケットC1, C2, C3, ……をハードディスク18から読み出して、暗号鍵K1, K2, K3, ……により復号化する。

【0090】

そして、テレビジョン放送受信機15は、復号化された動画パケットP1, P2, P3, ……を、図8(c)に示すように所定回数づつ繰り返し再生し、ここに、スロー再生が実現されることになる。

【0091】

なお、上記した実施の形態では、テレビジョン放送受信機15がインターネット19に送信する上りデータにタイムスタンプTiを指定する情報を含ませ、サーバ12は、上りデータで指定されたタイムスタンプTiとその暗号鍵Kiとを送信するようにしている。

【0092】

しかしながら、これに限らず、例えば、上りデータで再生や早送り再生等の機能のみを指定することにより、サーバ12が、要求された機能から自動的に必要とするタイムスタンプTiを選択して、暗号鍵Kiとともに送信するように構成してもよいものである。このようにすれば、テレビジョン放送受信機15における再生動作及びその他の特殊再生動作を、サーバ12側、つまり、コンテンツの提供者側で容易に管理することが可能となる。

【0093】

また、上記した実施の形態では、衛星14を介して放送される暗号化動画コンテンツを、予めテレビジョン放送受信機15で受信してハードディスク18に蓄積するようにしたが、ハードディスク18に蓄積する暗号化動画コンテンツとし

ては、例えば通信ネットワーク等を用いて予め時間をかけて送られてくるものであってもよいものである。

【0094】

さらに、上記した実施の形態では、放送局11からサーバ12に暗号鍵K_iを送って保持させるようにしたが、逆に、サーバ12から暗号鍵K_iを放送局11に送り、放送局11ではサーバ12から与えられた暗号鍵K_iを用いて、放送する動画パケットP_iに暗号化を施すようにしてもよいものである。

【0095】

また、放送局11とサーバ12とは、それぞれ別々の事業者によって運営されていても、また、同一事業者によって運営されていてもよく、要するに、暗号鍵K_iを相互間で高いセキュリティをもって伝送し得るように構成されていればよいものである。

【0096】

なお、この発明は上記した実施の形態に限定されるものではなく、この外その要旨を逸脱しない範囲で種々変形して実施することができる。

【0097】

【発明の効果】

以上詳述したようにこの発明によれば、ユーザのネットワーク接続環境に無関係に、大容量のデータコンテンツを実用的なレベルで安定に配信することを可能とした送信装置、受信装置及び受信方法を提供することができる。

【図面の簡単な説明】

【図1】

この発明の実施の形態を示すもので、動画コンテンツ配信システムの概略を説明するために示す図。

【図2】

同実施の形態における動画コンテンツを暗号化する手法を説明するために示す図。

【図3】

同実施の形態におけるサーバ及びテレビジョン放送受信機の詳細を説明するた

めに示すブロック構成図。

【図 4】

同実施の形態におけるサーバのメモリに暗号鍵とタイムスタンプとが対応付けられて記録されていることを説明するために示す図。

【図 5】

同実施の形態におけるユーザが所望の動画コンテンツを視聴する際の操作画面を説明するために示す図。

【図 6】

同実施の形態における再生と一時停止とが要求された場合の動作を説明するために示す図。

【図 7】

同実施の形態における早送り再生が要求された場合の動作を説明するために示す図。

【図 8】

同実施の形態におけるスロー再生が要求された場合の動作を説明するために示す図。

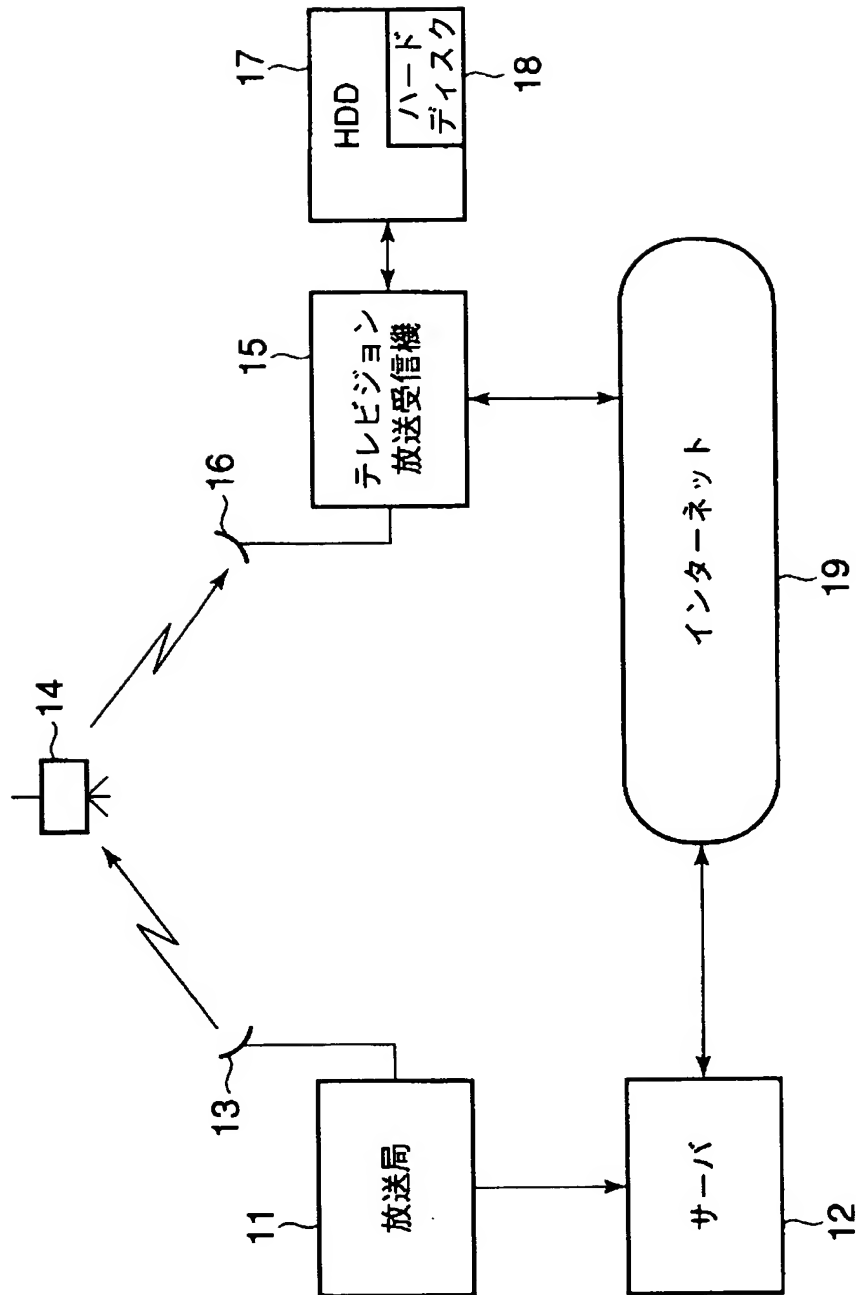
【符号の説明】

- 1 1 …放送局、
- 1 2 …サーバ、
- 1 3 …アンテナ、
- 1 4 …衛星、
- 1 5 …テレビジョン放送受信機、
- 1 6 …アンテナ、
- 1 7 …HDD、
- 1 8 …ハードディスク、
- 1 9 …インターネット、
- 2 0 …メモリ、
- 2 1 …制御部、
- 2 2 …読み出し部、

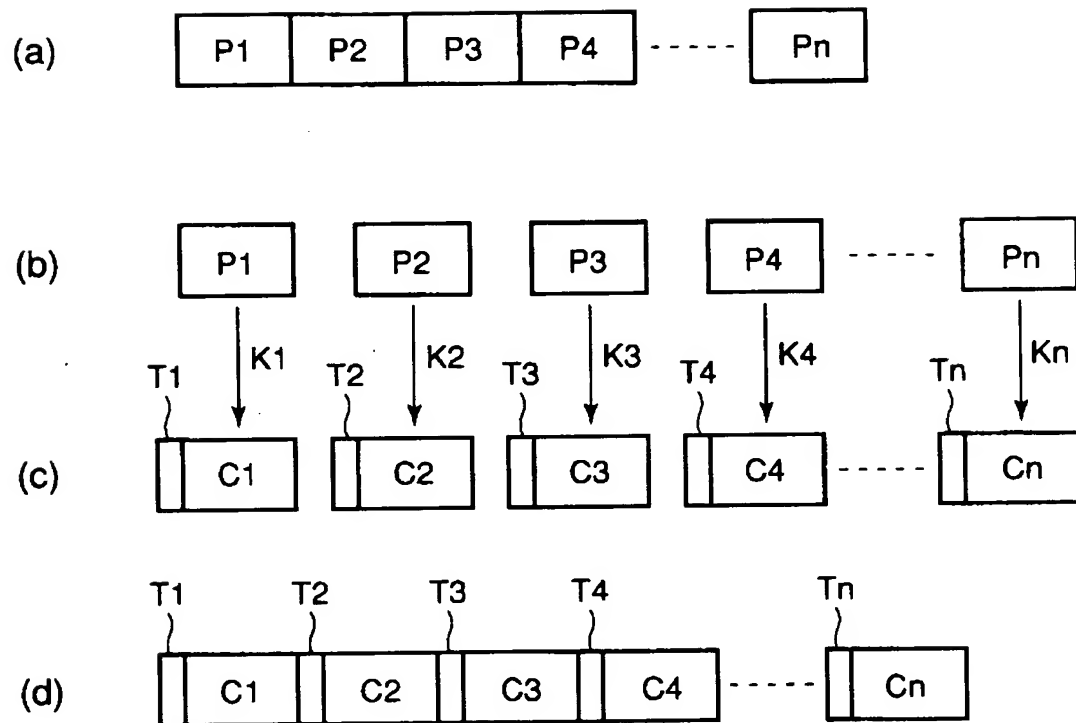
2 3 …エンコーダ、
2 4 …送信部、
2 5 …デコーダ、
2 6 …チューナ部、
2 7 …復調部、
2 8 …ファイルシステム部、
2 9 …リモートコントローラ、
3 0 …U I 部、
3 1 …エンコーダ、
3 2 …受信部、
3 3 …デコーダ、
3 4 …分離部、
3 5 …復号部、
3 6 …デコーダ、
3 7 …モニタ。

【書類名】 図面

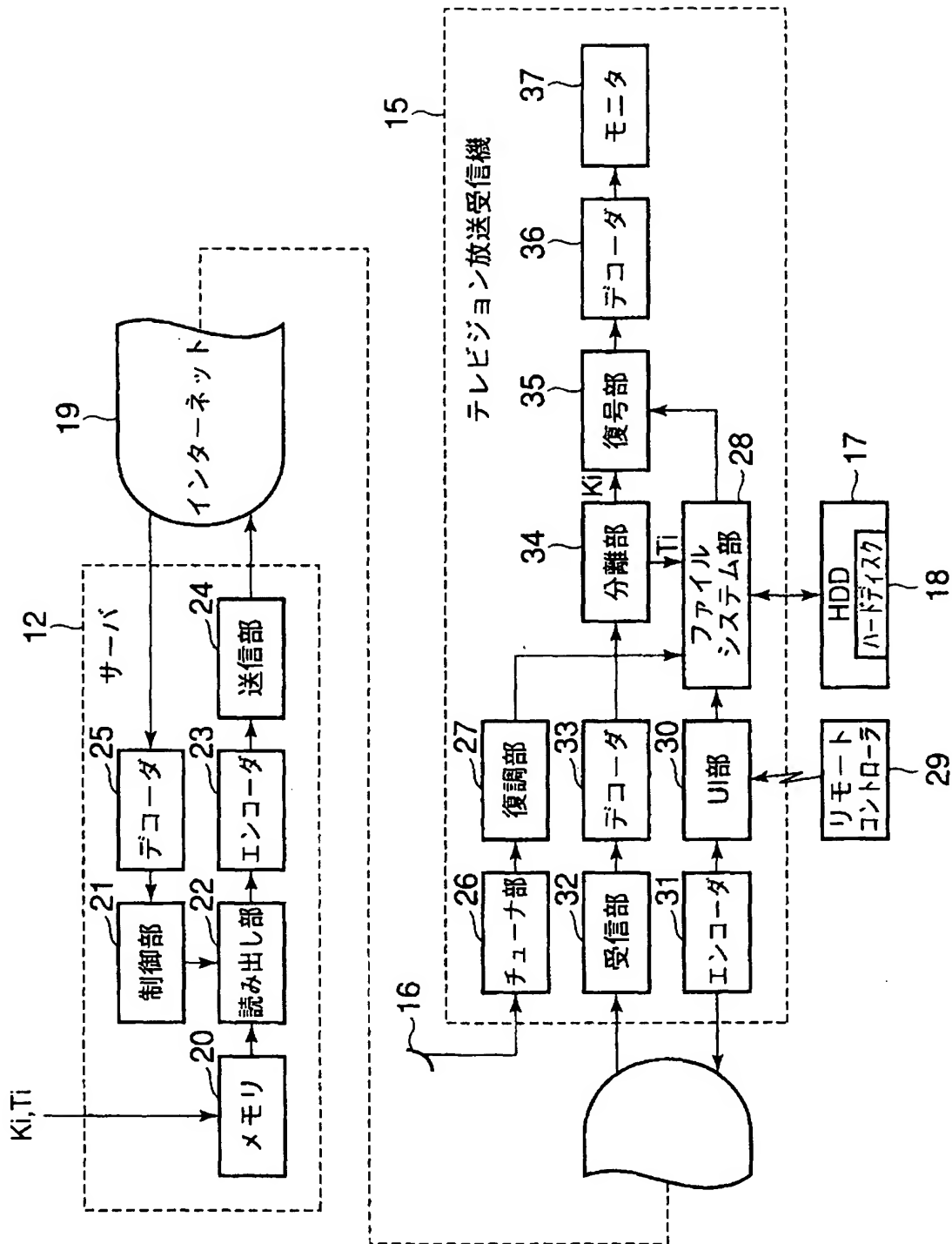
【図 1】



【図 2】



【図3】



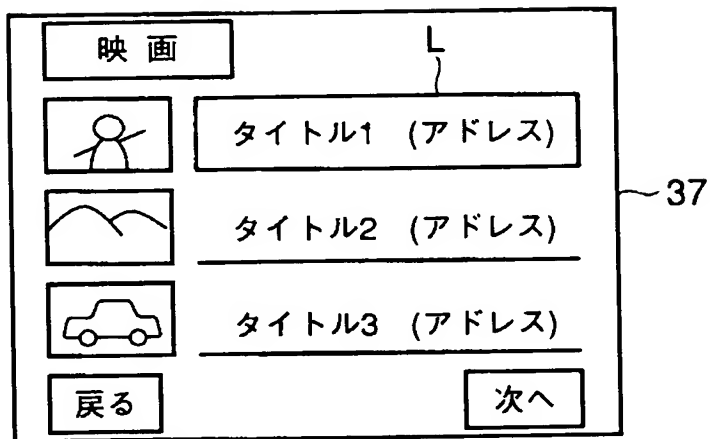
【図 4】

20

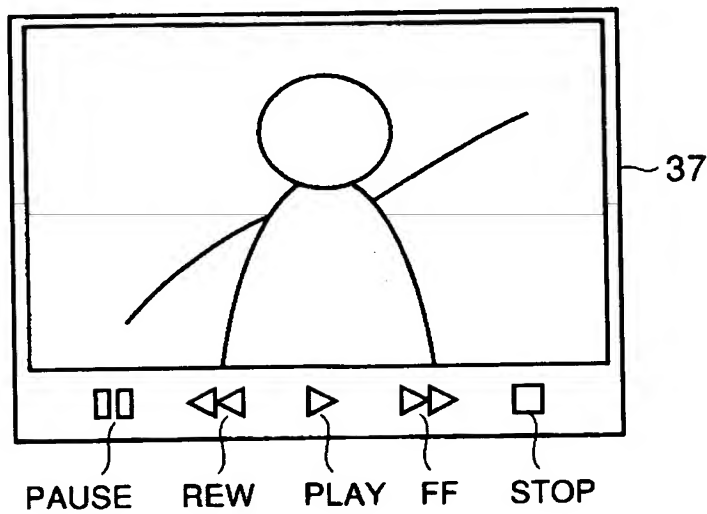
T1	K1
T2	K2
T3	K3
T4	K4
Tn	Kn

【図 5】

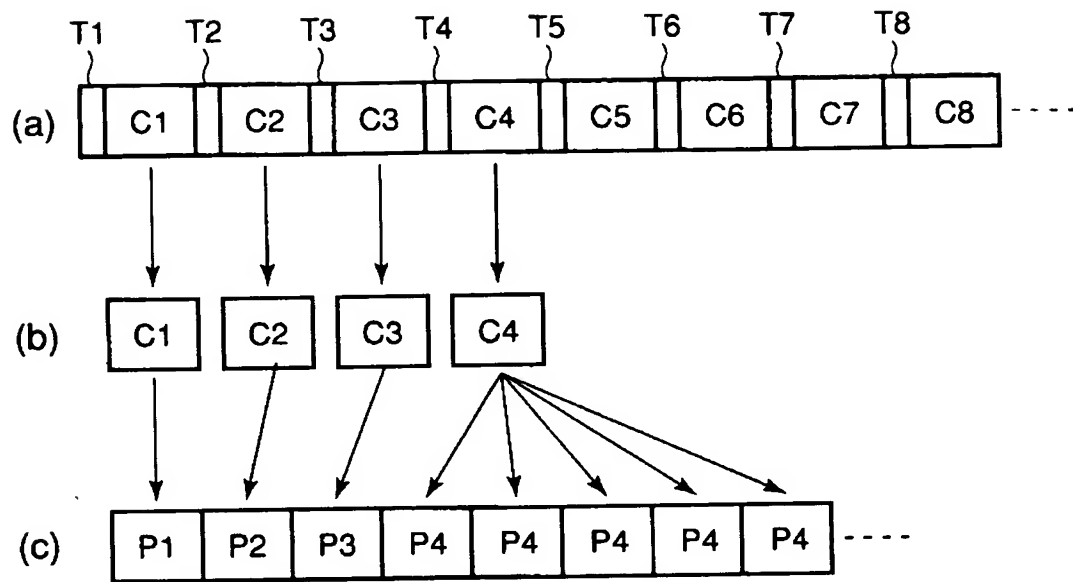
(a)



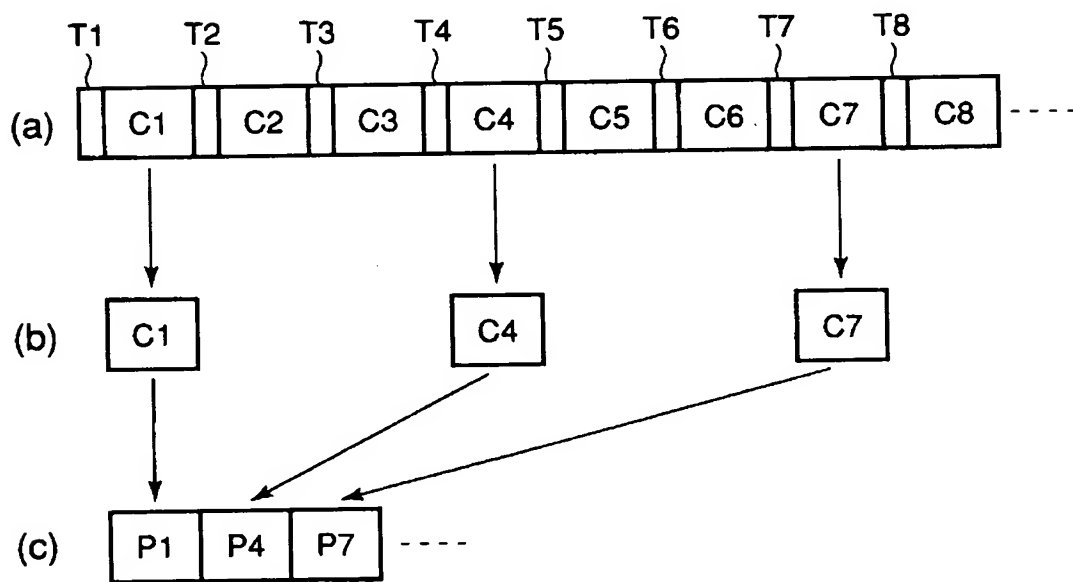
(b)



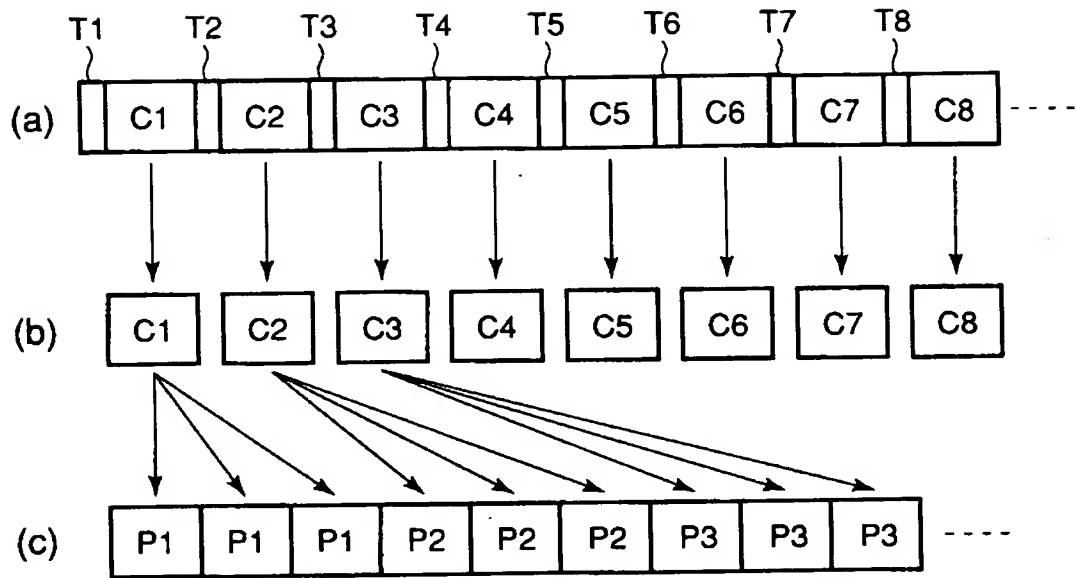
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】この発明は、ユーザのネットワーク接続環境に無関係に、大容量のデータコンテンツを実用的なレベルで安定に配信することを可能とした送信装置、受信装置及び受信方法を提供することを目的としている。

【解決手段】放送局 1 1 は、暗号化された動画コンテンツにリンク情報を付加して送信する。サーバ 1 2 は、暗号化動画コンテンツを復号するための暗号鍵を保持している。テレビジョン放送受信機 1 5 は、受信した暗号化動画コンテンツとリンク情報とをハードディスク 1 8 に蓄積し、リンク情報に基づいてインターネット 1 9 を介してサーバ 1 2 から暗号鍵を取得し、暗号化動画コンテンツを復号する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	2001年 7月 2日
[変更理由]	住所変更
住 所	東京都港区芝浦一丁目1番1号
氏 名	株式会社東芝